

Clase 1 — 02.10.25

#virtualbox

#ciscopackettracer

👤 Profesor: Carlos Quintana

💻 Unidad: Ciberseguridad

📅 Clase 1— 02/10/2025

🎯 Tema: Presentación de la asignatura e instalación del Virtualbox y configuracion de VM Windows Server

Clase 1 - Ciberseguridad DAM

📅 Tema: Instalación y configuración de Windows Server 2019 en VirtualBox + introducción a Cisco Packet Tracer

1. Objetivo de la asignatura

- Conocer herramientas de **seguridad informática** básicas.
- Entender el rol de un **servidor** en una red corporativa.
- Cisco Packet Tracer → aprender conexiones inalámbricas, cortafuegos y simulaciones de seguridad.
- ⚠️ En el máster de Ciberseguridad se estudiará con mayor detalle, aquí solo se verán **pinceladas introductorias**.

2. Cisco Packet Tracer

- Inicio de sesión:
 - Usar el **botón verde (Skills for All)** con el correo institucional.
- Conceptos que veremos:
 - **AAA (Authentication, Authorization, Accounting)**
 - **Autenticación** → Verifica la identidad del usuario.
 - **Autorización** → Define qué recursos puede usar.
 - **Contabilidad** → Registra las acciones realizadas.
 - **Cortafuegos:**
 - **Físicos (hardware de Cisco)**: dispositivos de seguridad dedicados, muy robustos y difíciles de vulnerar.
 - **Lógicos (software)**: protecciones que funcionan dentro del sistema operativo o aplicaciones.

📌 Empresas modernas utilizan **ambos tipos de firewall** para una defensa en profundidad.

mindmap

```
root((Seguridad en Redes))
```

```
AAA
```

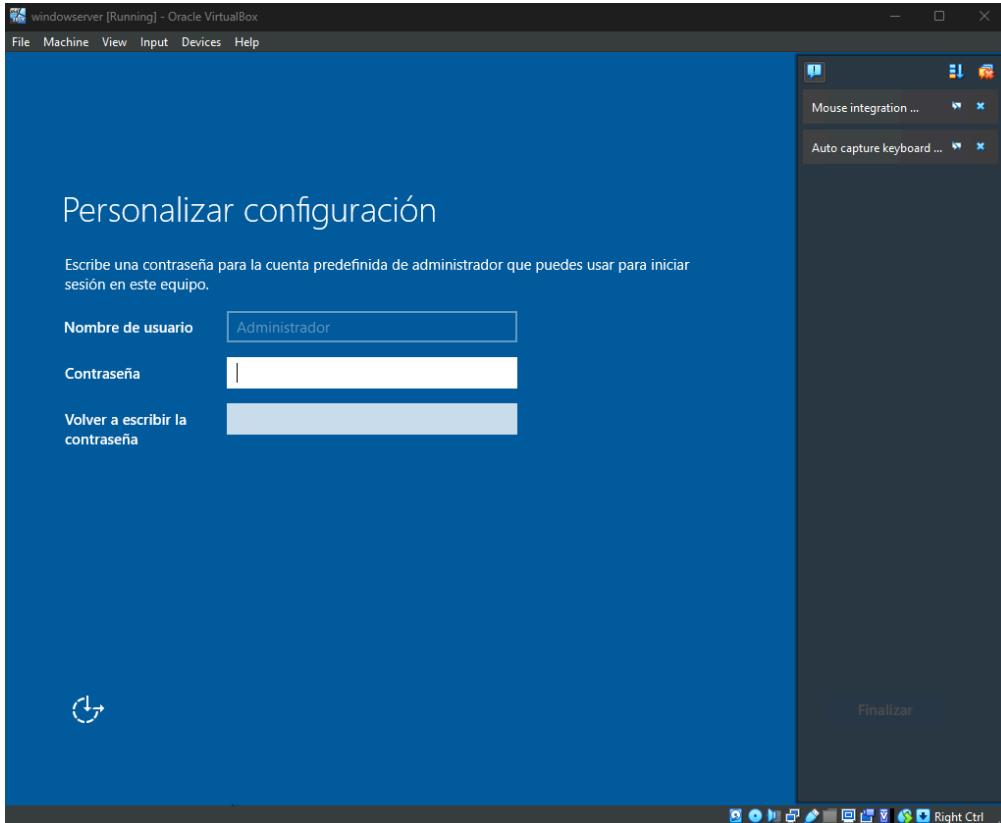
```
    Autenticación
```

```
        Verifica identidad del usuario
```

```
        Ej: Login con usuario y contraseña
```

Autorización	Define qué recursos puede usar el usuario
Ej: Acceso a carpetas, impresoras,	aplicaciones
Contabilidad	
Registra acciones del usuario	
Ej: Logs de acceso, auditorías	
Cortafuegos	
Físicos	
Dispositivo de hardware (Cisco ASA, Firepower)	
Difíciles de penetrar	
Usados en empresas	
Lógicos	
Software integrado en sistemas operativos	
Ej: Windows Defender Firewall, iptables en Linux	

3. Instalación de Windows Server 2019 en VirtualBox



usuario: administrador

Password: Adm123

- Al instalarlo por primera vez, Windows Server **no tiene roles de servidor activados** (parece un Windows normal).
- Para que funcione como **servidor real**, se deben agregar **roles y características**.
- El más importante para entornos empresariales: **Active Directory Domain Services (AD DS)**.

3.1. Estado inicial tras la instalación

- Cuando instalamos **Windows Server 2019** en VirtualBox, el sistema operativo se comporta **como un Windows normal**, sin funciones de servidor.
- Esto se debe a que, por defecto, no tiene instalados **roles ni características**.

- Es decir, al encenderlo solo veremos:
 - Escritorio clásico de Windows.
 - Explorador de archivos.
 - Herramientas administrativas básicas (Administrador del servidor, PowerShell, Panel de control).
- A este estado se le conoce como “**servidor sin roles**”.

💡 **Importante:** No es que sea “como Windows 95”, sino que simplemente **no cumple ninguna función de servidor** hasta que le agregamos roles.

3.2. Tipos de instalación posibles

Durante la instalación, se pueden elegir **dos variantes**:

1. Windows Server (Server Core):

- Instalación sin entorno gráfico (solo línea de comandos y PowerShell).
- Más seguro y ligero.
- Usado en entornos empresariales donde la administración se hace remotamente.

2. Windows Server (Desktop Experience):

- Instalación con entorno gráfico (GUI).
- Es la que usamos en clase porque facilita la práctica y visualización.
- Permite usar Administrador del Servidor y asistentes gráficos.

3.3. ¿Qué son los Roles y Características?

• Roles:

- Son las funciones principales que el servidor puede desempeñar.
- Ejemplos:
 - Active Directory Domain Services (AD DS).
 - DNS Server.
 - DHCP Server.
 - IIS (Servidor web).

• Características:

- Son complementos que añaden utilidades a los roles o al propio sistema.
- Ejemplos:
 - .NET Framework.
 - Herramientas de administración remota.
 - Servicios de respaldo (Windows Backup).

💡 Un Windows Server sin roles = un **sistema en blanco** que todavía no hace de servidor.

3.4. Instalación en VirtualBox

• Pasos básicos seguidos en clase:

1. Crear **máquina virtual** en VirtualBox.
 - Asignar nombre, 2-4 GB RAM, disco virtual de al menos 40 GB.
2. Montar la ISO de **Windows Server 2019**.

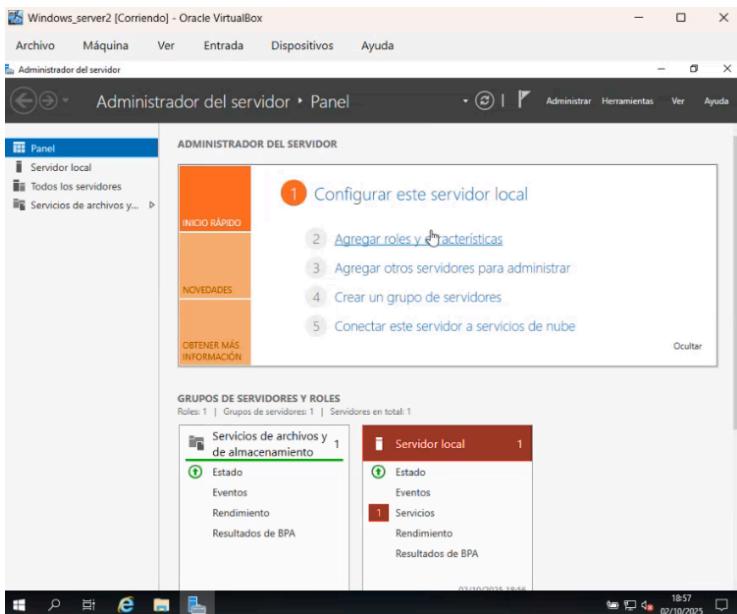
3. Instalar el sistema eligiendo la versión con **Desktop Experience**.
 4. Configurar usuario administrador y contraseña inicial.
 5. Iniciar sesión y acceder al **Administrador del servidor**, que se abre automáticamente.
-

3.5. Relación con la Ciberseguridad

- Un **servidor recién instalado** es **vulnerable**, porque:
 - No tiene roles de seguridad configurados.
 - No tiene cortafuegos ni políticas activas avanzadas.
- A partir de aquí, se agregan roles como **AD DS, DNS, DHCP** que permiten controlar:
 - Qué usuarios acceden a qué recursos.
 - Qué equipos forman parte del dominio.
 - Cómo se gestionan las políticas de seguridad.

4. Configuración de Windows Server

4.1. Promocionar a Controlador de Dominio



Pasos:

1. Abrir **Administrador del servidor**.
2. Ir a **Agregar roles y características**.
3. Seleccionar **Servicios de dominio de Active Directory (AD DS)**.
4. Tras la instalación, hacer clic en el ícono de la **bandera (notificación)**.
5. Seleccionar **Promover este servidor a controlador de dominio**.
6. Elegir **Agregar un nuevo Bosque** (ejemplo: `recursoshumanos.com`).
7. Configurar contraseña:
 - Contraseña de **Administrador de Dominio** (nivel superior al administrador local).
 - En este ejercicio, se recomienda usar la misma contraseña para no confundirse.

Resultado final:

- El servidor pasa de ser “un Windows normal” a un **Controlador de Dominio**.

- Puede **agrupar lógicamente equipos** y aplicar políticas centralizadas (usuarios, permisos, seguridad).
-

5. Conceptos clave

5.1. Controlador de dominio (Domain Controller)

- Es el **núcleo de una red corporativa basada en Active Directory (AD DS)**.
 - Su función principal es **autenticar y autorizar** a los usuarios y equipos que forman parte del dominio.
 - Permite centralizar la administración de usuarios, contraseñas, políticas y recursos compartidos.
-  En un entorno real, las empresas suelen tener **varios controladores de dominio** por seguridad y redundancia (uno principal y otro de respaldo).

Ejemplo:

Cuando un empleado inicia sesión en su PC corporativo, sus credenciales no se validan localmente, sino que son verificadas por el **controlador de dominio**. Si es correcto, el servidor permite el acceso a los recursos de la red (carpetas, impresoras, aplicaciones, etc.).

5.2. Active Directory (AD DS)

- **Active Directory Domain Services** es el rol más importante de Windows Server en el ámbito de la seguridad y la gestión de redes.
- AD DS organiza los elementos de la red en una **estructura jerárquica y lógica**.
- Esta estructura se compone de **Bosques, Dominios y Unidades Organizativas (UO)**.

Estructura jerárquica básica:

Bosque → Dominio → Unidades Organizativas (UO) → Usuarios, Grupos, Equipos

Ejemplo:

- Bosque: empresa.com
- Dominio: barcelona.empresa.com
- UO: RecursosHumanos , IT , Ventas

Cada UO puede tener sus propias políticas de seguridad, usuarios y permisos específicos.

5.3. Bosque (Forest)

- Es la **estructura más alta de Active Directory**.
- Representa el conjunto completo de todos los dominios, usuarios y recursos compartidos bajo una única infraestructura de seguridad.
- Todos los dominios dentro de un bosque **confían entre sí** automáticamente (confianza transitable).

Ejemplo:

El bosque empresa.com puede contener los dominios:

- ventas.empresa.com
- it.empresa.com
- recursoshumanos.empresa.com

Cada uno con sus propios controladores de dominio y políticas, pero bajo una misma jerarquía.



5.4. Dominio (Domain)

- Es una **agrupación lógica de usuarios, equipos y recursos** que comparten una misma base de datos de seguridad.
- Los dominios facilitan la **administración centralizada** mediante políticas y credenciales únicas.
- Cada dominio tiene un **nombre DNS único**, como `recursoshumanos.com`.

Ejemplo:

Todos los empleados de recursos humanos pueden iniciar sesión con una sola cuenta del dominio:

`usuario@recursoshumanos.com`

✳ 5.5. Unidad Organizativa (Organizational Unit - OU)

- Las **UO** sirven para organizar los objetos dentro de un dominio (usuarios, grupos, equipos).
- Permiten aplicar **políticas de grupo (GPO)** de manera específica según el departamento o función.

Ejemplo:

Dentro del dominio `empresa.com`, podemos crear:

- UO `SoporteIT` con políticas que permiten acceso a herramientas administrativas.
- UO `Finanzas` con restricciones de acceso a internet y permisos de lectura limitada.

🔑 5.6. Políticas de grupo (GPO - Group Policy Objects)

- Son **conjuntos de configuraciones de seguridad** que el administrador puede aplicar a usuarios o equipos dentro del dominio.
- Permiten controlar casi todo:
 - Contraseñas y bloqueos de sesión.
 - Instalación de programas.
 - Acceso a puertos USB.
 - Configuración del cortafuegos.
 - Scripts de inicio y apagado.

Ejemplo:

Una política puede establecer que todos los equipos del dominio bloqueen la sesión tras 5 minutos de inactividad o que no se puedan instalar aplicaciones externas.



5.7. Niveles de privilegio

- **Administrador local:** controla solo el equipo físico (por ejemplo, el servidor o un PC individual).
- **Administrador de dominio:** controla toda la red bajo ese dominio (usuarios, permisos, políticas).
- **Usuario estándar:** tiene acceso solo a los recursos que el administrador le haya autorizado.

Ejemplo:

El administrador de dominio puede crear o eliminar cuentas de usuario de toda la empresa, mientras que un usuario estándar solo puede cambiar su propia contraseña.



🌐 5.8. Importancia de mantener el servidor encendido

- El **controlador de dominio** debe estar **siempre activo**, ya que:
 - Gestiona la autenticación de los usuarios al iniciar sesión.
 - Controla el acceso a carpetas compartidas y recursos.
 - Ejecuta tareas programadas y políticas de seguridad.
 - Si el servidor está apagado, los equipos cliente **no podrán iniciar sesión en el dominio** (a menos que se haya guardado una caché temporal de credenciales).
-

5.9. Relación con la seguridad informática

- Centralizar la autenticación y las políticas en un servidor reduce la superficie de ataque.
- Permite:
 - Controlar contraseñas y permisos de todos los usuarios.
 - Aplicar políticas de seguridad coherentes en toda la red.
 - Monitorear actividad sospechosa mediante logs y auditorías.

 Este modelo de seguridad es **fundamental en entornos empresariales** y se combina con herramientas como firewalls, antivirus y sistemas de detección de intrusiones (IDS/IPS).

6. Práctica futura

- Trabajaremos con:
 - **Windows Server 2019** como **controlador de dominio**.
 - **Windows 10 Pro** como cliente, para probar políticas y autenticación.
 - Objetivo: **ver todas las herramientas de seguridad** que ofrece un entorno empresarial real.
-

 Final clase 1